Pers Ubiquit Comput (2015) 19:1053–1061
DOI 10.1007/s00779-015-0876-6

ORIGINAL ARTICLE

# C2MP: Chebyshev chaotic map-based authentication protocol for RFID applications

**Zhihua Zhang[1] · Huanwen Wang[1] · Yanghua Gao[1]**

Received: 15 December 2014 / Accepted: 1 May 2015 / Published online: 1 September 2015


**Abstract** Radio frequency identification (RFID) is a promising wireless sensor technology in the Internet of Things and can be applied for object identification. However, the security issues are still open challenges and should be addressed to achieve enhanced safeguard. Existing security solutions mainly apply logical operators, hash function, and other cryptographic primitives to design authentication schemes. In this paper, we propose a Chebyshev chaotic map-based authentication protocol (C2MP) for the RFID applications. Thereinto, Chebyshev polynomial's semigroup and chaotic properties are introduced for identity authentication and anonymous data transmission. The proposed C2MP owns the security properties including data integrity, authentication, anonymity, and session freshness. According to the BAN logic, security formal analysis is performed based on the messages formalization, initial assumptions, anticipant goals, and logic verification. It indicates that the proposed C2MP is suitable for universal RFID applications.

**Keywords** Radio frequency identification (RFID) · Authentication · Chebyshev chaotic map · Protocol · Security

## 1 Introduction

Radio frequency identification (RFID) is a promising wireless sensor technology in the Internet of Things (IoT) and can be applied for object identification in various applications such as supply chain, logistics, and asset management. Due to the open wireless communication channels, the reader–tag air interface is suffering from several security threats and attacks [1, 2]. Consequently, security issues become key concerns with the increasing popularity of RFID systems. It is necessary to propose an authentication scheme for security protection in the RFID applications.

In RFID systems, readers are deployed for distributed tag data acquirement, collection and extraction in wireless radio environments. The open environments during the system operations bring serious security challenges. Due to the tags are assigned with sensitive data involving a wide variety of applications from transportation, logistics, to asset management [3, 4]. Therefore, RFID systems differ from the traditional wireless systems, which suffer from more insecure situations and may be subject to more attacks for commercial purposes.

Several security solutions have been proposed to address potential security problems in RFID systems, including physical mechanisms, authentication protocols, access control protocols, and encryption algorithms. Thereinto, authentication protocols are the principal schemes that own ubiquitous applicability. There are three main categories of authentication protocols according to the weight of cryptographic primitives [13]. Concretely, the ultra-lightweight protocols mainly apply the bitwise logical operators and pseudo-random number generator (PRNG) to achieve safeguard [5–7]. The lightweight protocols mainly use cyclic redundancy code (CRC) operator, message authentication code (MAC), and hash function to realize identity authentication [8–11]. The middleweight protocols introduce the full-fledged symmetric/asymmetric encryption [e.g., elliptic curve cryptography (ECC)] for the applications with

✉ Zhihua Zhang
yhgao633@sohu.com

[1] China Tobacco Zhejiang Industrial Co., Ltd, Hangzhou, China

higher security requirements (e.g., finance, and military) [12–15]. However, several complicated protocols may be limited by the tag hardware requirements such as power consumption, storage space, and computational capacity. Hence, it is necessary to propose a suitable authentication scheme to achieve improved robustness, reliability and security. The existing security schemes are mainly based on the modern cryptography for different RFID applications. Recently, chaos encryption becomes an attractive direction to address security issues. Thereinto, Chebyshev chaotic map owns perfect randomness, semi-group and chaotic properties for the chaotic sequences, which can be introduced for identity authentication and anonymous transmission.

A sound security solution should achieve three main security requirements in RFID applications [16]. (1) *Authentication*: The readers and tags should pass the verification by the backend database so that any illegal reader cannot access the system for resource abuse, and any illegal tag cannot pass the verification for information cheat. (2) *Anonymity*: Both readers and tags should protect their own identifiers during ongoing communications, and attackers cannot obtain any sensitive information with privacy considerations. (3) *Session freshness*: The interactive session can be regarded as freshness due to the random operators, any attackers cannot correlate two communication sessions, and also cannot derive the previous or subsequent interrogations according to the current session.

In this work, we propose a Chebyshev chaotic map-based authentication protocol (C2MP) for RFID applications, and the main contributions are as follows.

- The semi-group property of Chebyshev chaotic map is introduced for authentication. The defined algebraic relationships of the Chebyshev polynomials are adopted to realize mutual trust relationship among the legal entities.
- The chaotic property of Chebyshev chaotic map is applied to enhance anonymous message transmission. An attacker cannot obtain any sensitive information of the ongoing session due to irregular message flows.
- The pseudo-random numbers are adopted to enhance the randomization and forward security of the interactions, and session freshness is achieved to against a typical attack such as replay attack.

The remainder of the paper is organized as follows. Section 2 introduces the related works in RFID security. Section 3 reviews the proposed authentication protocol. Sections 4 and 5 present the security formal analysis and performance analysis. Finally, Sect. 6 draws a conclusion.

## 2 Related work

Tian et al. [5] proposed an ultralightweight RFID authentication protocol with permutation (RAPP), which avoids to apply the unbalanced OR and AND operations for authentication. In the RAPP, the tags only perform the bitwise XOR, left rotation and permutation operations. Meanwhile, de-synchronization attacks are addressed by the unique message transmission mode. According to the security analysis, the RAPP satisfies the main security properties to defend the various attacks.

Liu et al. [6] proposed a grouping-proofs based authentication protocol (GUPA) to address the security issue for multiple readers and tags simultaneous identification in distributed RFID systems. In the GUPA, distributed authentication mode with independent subgrouping proofs is adopted to enhance hierarchical protection, an asymmetric denial scheme is applied to grant fault-tolerance capabilities against an illegal reader or tag, and a sequence based odd-even alternation group subscript is presented to define a function for secret updating. It indicates that the GUPA realizing both secure and simultaneous identification is efficient for the resource constrained distributed RFID systems.

Liu and Ning [7] proposed a zero-knowledge authentication protocol (ZKAP) based on alternative mode for RFID systems. In the ZKAP, dual zero-knowledge proofs are randomly chosen to provide anonymity and mutual authentication without revealing any sensitive identifiers. Pseudo-random flags and access lists are employed for quick check to ensure high efficiency and scalability. It indicates that the ZKAP owns no obvious design defects theoretically and is robust enough to resist the forgery, replay, Man-in-the-Middle (MITM), and tracking attacks.

Liu et al. [8] proposed a lightweight mutual authentication protocol based on variable linear feedback shift registers for EPC Gen2 standard systems. An application specific integrated circuit (ASIC) implementation of the protocol is performed with low-power consumption.

Yao et al. [9] proposed a multiple tags privacy-preserving authentication protocol (MAP) for authenticating a batch of tags with strong privacy and high efficiency. The MAP applies batch-type authentication pattern, and leverages the collaboration among multiple tags for accelerating the authentication speed. Both security protection and privacy preservation are achieved in terms of confidentiality, cloning resistance, tracking resistance, timing-based attack resistance, and forward secrecy.

Morshed et al. [11] proposed an efficient mutual authentication protocol by using individual secret values for each tag. This protocol avoids complex hash operations in the database to reduce the computation overhead. The

evaluation indicates that the protocol requires a low tag storage, computation and communication cost for lightweight RFID applications.

Toward Chebyshev chaotic map-based authentication protocols, Ning et al. [17] proposed an aggregated-proof based hierarchical authentication scheme (APHA) for the unit IoT and ubiquitous IoT. In the APHA, the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; and directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication. Particularly, Chebyshev chaotic maps are applied to describe the mapping relationships between the shared secrets and the path descriptors for mutual authentication.

In this work, we propose an RFID authentication protocol absorbing the merits of former schemes based on lightweight bitwise operations. Compared with the existing researches, the proposed C2MP based on the semi-group property and chaotic property of Chebyshev chaotic map differs from the conventional security scheme applying complex hash function and cryptographic algorithms. Considering the limitations of tags, the proposed C2MP based on algebraic and bitwise operations is suitable for ubiquitous systems in pervasive computing environments. The combination of Chebyshev chaotic map, hash function, pseudo-random numbers, and mutual authentication mechanism has not received much attention from previous studies.

## 3 The proposed authentication protocol

### 3.1 System initialization

In the RFID system, there are readers, tags, and a backend database. The communication between a reader and the database can be regarded as a secure channel, while the communication link between a reader and a tag is suffering from various security attacks and threats. Assume that a reader ($R$) and a tag ($T$) own the corresponding pseudonyms $PID_R$ and $PID_T$, the database ($DB$) owns all the legal readers and tags information and a pre-shared value $Q \equiv \mathcal{T}_x(S) \pmod{p}$, in which $x \in \mathbb{Z}^*$ is a secret value, $S$ is a pre-shared value, and $p$ is a large prime. Both $T$ and $R$ own the values $\{Q, S, p\}$. The detailed notations are introduced in Table 1.

In the system initialization, hardware and software requirements are given as follows [13].

- Tags considered in the system are smart cards comprising an intelligent micro-processor unit (MPU), storage units and chip operating system (COS). Assume that tags have the basic crypto-operational and storage capabilities to realize data transmission in the open channels.
- Readers are static or mobile active devices distributed to cover the areas where tags exit. Both the readers and the database are not power constrained, and besides the database is regarded as the credible entity.
- The communication channel between a reader and the back-end database is assumed to be secure, while the wireless channel between a reader and a tag is vulnerable.

**Table 1** Notations

| Notation | Description |
|---|---|
| $R$, $T$, $DB$ | The reader, tag, and database |
| $PID_R, PID_T$ | The reader/tag's pseudonym |
| $r_R, r_T$ | The reader/tag's pseudo-random numbers |
| $TID_R, TID'_R$ | The reader's temp pseudonym |
| $TID_T, TID'_T, TID''_T$ | The tag's temp pseudonym |
| $S$, $Q$ | The pre-shared value for the legal entities |
| $x$, $y$, $z$ | The random integers |
| $\mathcal{T}_*(.)$ | The Chebyshev polynomial |
| $H(.)$ | The hash function |
| $\|\|$ | The comparison operator |
| $\rightarrow$ | The transition operator |

Note that the physical destructions such as removing a tag physically from a tagged item are not considered since there are no technical methods to discriminate between intentional or unintentional behaviors.

The Chebyshev chaotic maps is available for authentication [18, 19]. Suppose that a Chebyshev polynomial $\mathcal{T}_x(m)$ is in $x$ of degree $m$, and $\mathcal{T}_x(m) : [-1, 1] \rightarrow [-1, 1]$ is defined as follows:

$$\mathcal{T}_x(m) = \cos(l \cdot \arccos(m))$$

The Chebyshev polynomials satisfy the following relationships.

$$\mathcal{T}_0(m) = 1,$$
$$\mathcal{T}_1(m) = m,$$
$$\mathcal{T}_x(m) = \cos(l \cdot \arccos(m)); \quad (l \geq 2).$$

Define the degrees $\{x_1, x_2\}$ are positive integer numbers. The Chebyshev polynomials $\mathcal{T}_{x_1}(m)$ and $\mathcal{T}_{x_2}(m)$ ($m \in [-\infty, \infty]$) are assigned with the semigroup and chaotic properties.

$$\mathcal{T}_x(m) \equiv (2m\mathcal{T}_{l-1}(m) - \mathcal{T}_{x-2}(m)) \pmod{q}; \quad (l \geq 2),$$
$$\mathcal{T}_{x_1}(\mathcal{T}_{x_2}(m))$$

In the trust model, $DB$ is an only entity trusted by all the readers and tags. There is no other direct trust relationships

between readers and tags. Thereinto, a reader is assigned with default access authority on a set of tags.

### 3.2 The protocol descriptions

An interaction among $\{R, T, DB\}$ is introduced to describe the protocol process. Figure 1 shows the proposed Chebyshev chaotic map-based authentication protocol, and the main message exchanges among $R$, $T$, and $DB$ are as follows.

#### 3.2.1 Challenge–response between a reader and a tag

The reader $R$ generates a pseudo-random number $r_R$ and transmits $r_R$ to $T$ as an access challenge to launch a new session. Upon receiving the message, $T$ first generates a pseudo-random number $r_T$, and a random integer $z$. Thereafter, $T$ extracts the pre-shared values $\{Q, S\}$ and its pseudonym $PID_T$ to compute the authentication operators $\{A_T, B_T\}$, a temp identifier $TID_T$, and a hash value $H_T$.

$$\begin{aligned} A_T &= \mathcal{T}_z(S) \pmod{\text{p}},\\ B_T &= \mathcal{T}_z(Q) \pmod{\text{p}},\\ TID_T &= PID_T \oplus H(B_T \| r_T),\\ H_T &= H(TID_T \| B_T \| r_R). \end{aligned}$$

$T$ transmits the cascade messages $r_T \| A_T \| TID_T \| H_T$ to $R$ as a response. Upon receiving the messages, $R$ also generates a random integer $y$. Afterward, $R$ computes its authentication operators $\{A_R, B_R\}$, a temp identifier $TID_R$, and a hash value $H_R$.

$$\begin{aligned} A_R &= \mathcal{T}_y(S) \pmod{\text{p}},\\ B_R &= \mathcal{T}_y(Q) \pmod{\text{p}},\\ TID_R &= PID_R \oplus H(B_R \| r_R),\\ H_R &= H(TID_R \| B_R \| r_T). \end{aligned}$$

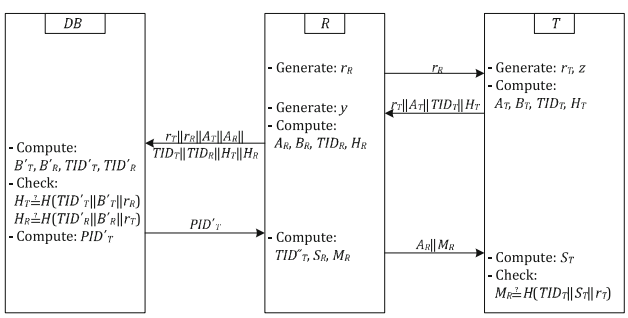


**Fig. 1** The Chebyshev chaotic map-based authentication protocol

#### 3.2.2 Authentication on both reader and tag by the database

$R$ transmits the cascade messages $r_T \| A_T \| TID_T \| H_T$ and $r_R \| A_R \| TID_R \| H_R$ to the database $DB$ for authentication. Upon receiving the messages, $DB$ extracts the locally stored pseudonyms $\{PID_T, PID_R\}$ to compute the values $\{B'_T, B'_R\}$ and the temp identifier $\{TID'_T, TID'_R\}$, respectively, for $\{R, T\}$.

$$\begin{aligned} B'_T &= \mathcal{T}_x(A_T) \pmod{\text{p}},\\ B'_R &= \mathcal{T}_x(A_R) \pmod{\text{p}},\\ TID'_T &= PID_T \oplus H(B'_T \| r_T),\\ TID'_R &= PID_R \oplus H(B'_R \| r_R). \end{aligned}$$

According to $Q \equiv \mathcal{T}_x(S) \pmod{\text{p}}$, it turns out that $B'_T = B_T$ will hold.

$$\begin{aligned} B'_T &= \mathcal{T}_x(A_T) \pmod{\text{p}} = \mathcal{T}_x(\mathcal{T}_z(S)) \pmod{\text{p}},\\ B_T &= \mathcal{T}_z(Q) \pmod{\text{p}} = \mathcal{T}_z(\mathcal{T}_x(S)) \pmod{\text{p}}. \end{aligned}$$

Similarly, $B'_R = B_R$ can also be obtained since $\mathcal{T}_y(\mathcal{T}_x(S)) \pmod{\text{p}}$ theoretically equals $\mathcal{T}_x(\mathcal{T}_y(S)) \pmod{\text{p}}$.

$DB$ checks the validity of $\{T, R\}$ by computing the hash values $H(TID'_T \| B'_T \| r_R)$ and $H(TID'_R \| B'_R \| r_T)$, and compares whether the received values $\{H_T, H_R\}$ equal the computed values. If $H_T = H(TID'_T \| B'_T \| r_R)$ and $H_R = H(TID'_R \| B'_R \| r_T)$ hold, $DB$ will regard $T$ and $R$ as legal entities; otherwise, the protocol will terminate.

$DB$ further computes a value $PID'_T$, and transmits $PID'_T$ to $R$.

$$PID'_T = TID'_T \oplus H(B'_R \| r_R)$$

#### 3.2.3 Authentication on the reader by the tag

Upon receiving the messages, $R$ computes the temp identifier $TID''_T$, an authentication operator $S_R$, and a hash value $M_R$. $R$ transmits the cascade messages $A_R \| M_R$ to $T$ for further authentication.

$$\begin{aligned} TID''_T &= PID'_T \oplus H(B_R \| r_R),\\ S_R &= \mathcal{T}_y(A_T) \pmod{\text{p}},\\ M_R &= H(TID''_T \| S_R \| r_T). \end{aligned}$$

Thereafter, $T$ computes a value $S_T$ and checks the validity of $R$ by re-computing the hash value $H(TID_T \| S_T \| r_T)$. According to $Q \equiv \mathcal{T}_x(S) \pmod{\text{p}}$, it turns out that $S_T = S_R$ since $\mathcal{T}_z(\mathcal{T}_y(S)) \pmod{\text{p}} = \mathcal{T}_y(\mathcal{T}_z(S)) \pmod{\text{p}}$. If $M_R = H(TID_T \| S_T \| r_T)$ holds, $T$ will regard $R$ as a legal reader; otherwise, the protocol will terminate.

$$S_T = \mathcal{T}_z(A_R) \pmod{\text{p}}$$

Till now, $R$, $T$ and $DB$ have established the trusting relationships, and $DB$ has authenticated $\{R, T\}$ as legal entities. The Chebyshev chaotic map is applied for authentication, and the main authentication phases can be described as follows:

- $R \rightarrow T$: $r_R$;
- $T \rightarrow R$: $r_T \| A_T \| TID_T \| H_T$;
- $R \rightarrow DB$: $r_T \| A_T \| TID_T \| H_T, r_R \| A_R \| TID_R \| H_R$;
- $DB \rightarrow R$: $PID'_T$;
- $R \rightarrow T$: $A_R \| M_R$.

### 3.3 Security properties

The proposed C2MP is based on Chebyshev polynomials to adopt authentication, anonymity, and session freshness mechanisms to enhance security protection in the RFID systems.

#### *3.3.1 Authentication*

The authentication mechanism is applied to establish the mutual trusting relationships between interactive entities. Thereinto, the database $DB$ can be regarded as a trusted entity in the system. Note that the semigroup property of the Chebyshev polynomials is introduced for authentication, and the detailed authentication includes the following aspects:

- The database $DB$ performs authentication on both reader $R$ and tag $T$ by checking whether the received values $\{H_T, H_R\}$ equal the computed hash values $H(TID'_T \| B'_T \| r_R)$ and $H(TID'_R \| B'_R \| r_T)$. According to $Q \equiv \mathcal{T}_x(S) \pmod p$, it turns out that $B'_T = B_T$ and $B'_R = B_R$ will hold.
- The tag $T$ performs authentication on the reader $R$ by checking the consistency of the received $M_R$ and the re-computing the hash value $H(TID_T \| S_T \| r_T)$. It turns out that $S_T = S_R$ since $\mathcal{T}_z(\mathcal{T}_y(S)) \pmod p = \mathcal{T}_y(\mathcal{T}_z(S)) \pmod p$ holds.

#### *3.3.2 Anonymity*

The pseudonyms $\{PID_R, PID_T\}$ are wrapped along with the hash function, and the temp identifiers $\{TID_T, TID'_T, TID''_T\}$ and $\{TID_R, TID'_R\}$ are transmitted instead of the pseudonyms. The anonymous transmission mode makes that any attacker cannot obtain the real identifiers during the authentication process. Moreover, the polynomial's chaotic property enhances the anonymity due to the irregular message flow.

Meanwhile, data integrity is also achieved by one-way hash functions to guarantee that the interactive data cannot be modified during the authentication process.

- The tag's temp identifiers $\{TID_T, TID'_T, TID''_T\}$ and reader's temp identifiers $\{TID_R, TID'_R\}$ are computed by wrapping the pseudonyms $PID_T$ and $PID_R$ with the hash values $H(B_* \| r_*)$ and $H(B'_* \| r_*)$.
- The values $\{H_T, H_R, M_R\}$ are respectively computed by hashing the values $TID_T \| B_T \| r_R$ and $TID_R \| B_R \| r_T$.

Such hash values realize that any attacker cannot derive the sensitive information even if it obtains the exchanged messages via the open channels. The authentication protocol considers the channel limitations and applies lightweight hash functions in the wireless networks to realize the trade-off of security and efficiency.

#### *3.3.3 Session freshness*

Session freshness is achieved by introducing pseudo-random numbers, which also enhance the randomization and forward security.

- The pseudo-random numbers $r_R$ and $r_T$ are generated by the pseudo-random number generator (PRNG) and are used to compute the temp identifiers and hash values such as $\{TID_*, TID'_*, H_*, M_R\}$.
- The random integers $x$, $y$ and $z$ are generated to determine the degree of the Chebyshev polynomial $\mathcal{T}_*(.)$, which is applied for further authentication.

The current security compromises cannot correlate with the previous interactions due to the pseudo-random numbers.

## 4 Security formal analysis with BAN logic

In this section, Burrows–Abadi–Needham (i.e., BAN) logic [20] is applied to analyze the design correctness of the C2MP. The BAN logic is a rigorous evaluation method to detect subtle defects for authentication protocols. The security formal analysis focuses on belief and freshness, and involves the following steps:

1. Formalization of the protocol messages;
2. Declaration of initial assumptions;
3. Declaration of anticipant goals;
4. Verification by logical rules and formulas.

The main reasoning progress is based on the belief use postulates and definitions to determine whether the protocol goals can be derived from the initial assumptions and message exchanges. If such derivation exists, the protocol

**Table 2** The formal notations [20]

| Notation | Description |
|---|---|
| $P\|\equiv X$ | $P$ believes $X$, or $P$ would be entitled to believe $X$ |
| $P\triangleleft X$ | $P$ sees $X$. A party has sent a message containing $X$ to $P$ who can read and repeat $X$ |
| $P\|\sim X$ | $P$ once said $X$. $P$ sent a message including the statement $X$ before, and $P$ believed $X$ when he sent the message |
| $P\|\Rightarrow X$ | $P$ has jurisdiction over $X$. $P$ is an authority on $X$ and should be trusted on this matter |
| $\sharp(X)$ | $X$ is fresh, and $X$ has not been sent in a message at any time before the current run of the protocol |
| $P\overset{X}{\longleftrightarrow}P'$ | $X$ is a secret known only to $P$ and $P'$, and trusted by them. Only $P$ and $P'$ may use $X$ to prove their identities to each other |
| $\{X\}_Y$ | $X$ is combined with the formula $Y$. It means that $Y$ is a secret and that its presence prove the identity of whoever utters $\{X\}_Y$ |

will be regarded as reasonable. Table 2 shows formal notations in the BAN logic.

### 4.1 Message formalization

According to the authentication phases of the C2MP, the formalized messages (M) delivered among $R$, $T$ and $DB$ can be described in the following forms.

- M1 ($R\rightarrow T$): $T\triangleleft r_R$.

  $T$ receives $r_R$ from $R$, and can repeat $r_R$.

- M2 ($T\rightarrow R$): $R\triangleleft r_T, R\triangleleft A_T, R\triangleleft TID_T, R\triangleleft H_T$.

  $R$ receives $r_T\|A_T\|TID_T\|H_T$ from $T$ and can repeat the messages.

- M3 ($R\rightarrow DB$): $DB\triangleleft r_T, DB\triangleleft A_T, DB\triangleleft TID_T$, $DB\triangleleft H_T, DB\triangleleft r_R, DB\triangleleft A_R, DB\triangleleft TID_R, DB\triangleleft H_R$.

  $DB$ receives $r_T\|A_T\|TID_T\|H_T$ and $r_R\|A_R\|TID_R\|H_R$ from $R$ and can repeat the messages.

- M4 ($DB\rightarrow R$): $R\triangleleft PID'_T$.

  $R$ receives $PID'_T$ from $DB$, and can repeat the messages.

- M5 ($R\rightarrow T$): $T\triangleleft A_R, T\triangleleft M_R$.

  $T$ receives $A_R\|M_R$ from $R$, and can repeat the messages.

### 4.2 Initial assumptions

The initial possessions and abilities of each participant are defined, and the initiative assumptions (IA) can be obtained as follows.

- For $T$:

  IA1.1: $T|\equiv R\overset{S,Q,p}{\Longleftrightarrow}T$,
  IA1.2: $T|\equiv DB\overset{PID_T}{\Longleftrightarrow}T$,
  IA1.3: $T|\equiv\sharp(r_T,z)$,
  IA1.4: $T|\equiv DB|\Rightarrow(PID_T,x)$.

  IA1.1: $T$ believes that the secrets $\{S, Q, p\}$ are shared with $R$;
  IA1.2: $T$ believes that the pseudonym $PID_T$ is shared with $DB$;
  IA1.3: $T$ believes that the values $\{r_T, z\}$ are fresh and have never been sent before the current session;
  IA1.4: $T$ believes that $DB$ has jurisdiction over the values $\{PID_T, x\}$.

- For $R$:

  IA2.1: $R|\equiv T\overset{S,Q,p}{\Longleftrightarrow}R$,
  IA2.2: $R|\equiv DB\overset{PID_R}{\Longleftrightarrow}R$,
  IA2.3: $R|\equiv\sharp(r_R,y)$,
  IA2.4: $R|\equiv DB|\Rightarrow(PID_R,x)$.

  IA2.1: $R$ believes that the secrets $\{S, Q, p\}$ are shared with $T$;
  IA2.2: $R$ believes that the pseudonym $PID_R$ is shared with $DB$;
  IA2.3: $R$ believes that the values $\{r_R, y\}$ are fresh, and have never been sent before the current session;
  IA2.4: $R$ believes that $DB$ has jurisdiction over the values $\{PID_R, x\}$.

- For $DB$:

  IA3.1: $DB|\equiv T\overset{PID_T}{\Longleftrightarrow}DB$,
  IA3.2: $DB|\equiv R\overset{PID_R}{\Longleftrightarrow}DB$,
  IA3.3: $DB|\equiv T|\Rightarrow(PID_T,z)$,
  IA3.4: $DB|\equiv R|\Rightarrow(PID_R,y)$.

  IA3.1: $DB$ believes that the pseudonym $PID_T$ is shared with $T$;
  IA3.2: $DB$ believes that the pseudonym $PID_R$ is shared with $R$;
  IA3.3: $DB$ believes that $T$ has jurisdiction over the values $\{PID_T, z\}$;
  IA3.4: $DB$ believes that $R$ has jurisdiction over the values $\{PID_R, y\}$;

### 4.3 Anticipant goals

The main objectives are the data belief and freshness $R$, $T$ and $DB$. It guarantees that the messages are from trustable entities and were not used in former sessions. The anticipant goals (G) can be obtained as follows.

G1: $T|\equiv R|\sim PID_T$,

G2: $T| \equiv \sharp(M_R)$,
G3: $T| \equiv DB \overset{PID_R}{\Longleftrightarrow} R$,
G4: $R| \equiv DB \overset{PID_T}{\Longleftrightarrow} T$,
G5: $R| \equiv \sharp(H_T)$,
G6: $DB| \equiv T| \sim Q$,
G7: $DB| \equiv R| \sim Q$.

G1: $T$ believes that $R$ once sent a message including the statement $PID_T$;

G2: $T$ believes that the message $M_R$ is fresh, i.e., $T$ believes that $M_R$ has not been sent in a message at any time before the current run of the protocol;

G3: $T$ believes the pseudonym $PID_R$ is shared as a secret by $DB$ and $R$;

G4: $R$ believes the pseudonym $PID_T$ is shared as a secret by $DB$ and $T$;

G5: $R$ believes that the message $H_R$ is fresh;

G6: $DB$ believes that $T$ once sent a message including the statement $Q$;

G7: $DB$ believes that $R$ once sent a message including the statement $Q$.

Thereinto, G1, G3, G4, G6 and G7 refer to the belief requirements, and messages are sent from the legal participants instead of malicious attackers. G2 and G5 indicate freshness requirements. The received messages were not used by malicious attackers in the previous sessions.

### 4.4 Logic verification

The logic verification is performed based on the message formalization, initial assumptions, and BAN logic rules.

**Theorem 1** *$T$ believes that $R$ once sent a message including the statement $PID_T$.*

*Proof* According to M5: $T \triangleleft A_R, T \triangleleft M_R$, it turns out that $T$ has received messages $A_R$ and $M_R$. Thereinto, $A_R$ is a Chebyshev polynomial $\mathcal{T}_y(.)$ containing $S$, and $M_R$ is a hash value involving $TID''_T, S_R$ and $r_T$.

Here, $TID''_T$ is a temp value computed by introducing $TID'_T$, which theoretically equals $TID_T = PID_T \oplus H(B_T \| r_T)$. Thus, $T \triangleleft M_R$ can be regarded as follows, in which $*$ means omitted parameters.

$$T \triangleleft (\langle PID_T \rangle_Q, *)$$

Applying the seeing rule (R1): $\frac{P \triangleleft (X,Y)}{P \triangleleft X}$, we obtain that a party has sent a message containing $\langle PID_T \rangle_Q$ to $T$.

$$T \triangleleft \langle PID_T \rangle_Q$$

According to IA1.1: $T| \equiv R \overset{S,Q,p}{\longleftrightarrow} T, T$ believes that the secrets $\{S, Q, p\}$ are shared with $R$. Applying the message-meaning rule (RM3): $\frac{P| \equiv P' \overset{Y}{\longleftrightarrow} P, P \triangleleft \langle X \rangle_Y}{P| \equiv P'| \sim X}$, we obtain that:

$$T| \equiv R| \sim PID_T$$

If $T$ believes that $Q$ is a shared secret with $R$, and $T$ receives $\langle PID_T \rangle_Q, T$ will believe that $R$ once conveyed the message $PID_T$. Till now, G1 has been proven.

**Theorem 2** *$T$ believes that the message $M_R$ is fresh.*

*Proof* According to M5: $T \triangleleft M_R$, it turns out that $T$ has received messages $M_R$, which is a hash value involving $TID''_T, S_R$ and $r_T$. Thus, $T \triangleleft M_R$ can be regarded as follows.

$$T \triangleleft (r_T, *)$$

According to IA1.3: $T| \equiv \sharp(r_T), T$ believes that $r_T$ is fresh. Applying the freshness rule (F1): $\frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X,Y)}$, we obtain that:

$$T| \equiv \sharp(r_T, *)$$

If one part of $M_R$ (marked as $(r_T, *)$) is known to be fresh, then $M_R$ are also fresh. Thus, $T$ will believe that the message $M_R$ is fresh, and G2 has been proven.

**Theorem 3** *$T$ believes the pseudonym $PID_R$ is shared as a secret by DB and R.*

*Proof* $DB$ can be regarded as a secure entity during the interactions, and we obtain that:

$$T| \equiv DB| \Rightarrow (DB| \equiv *),$$
$$T| \equiv DB| \equiv (DB| \equiv *).$$

According to IA3.2: $DB| \equiv R \overset{PID_R}{\Longleftrightarrow} DB, DB$ believes that the pseudonym $PID_R$ is shared with $R$. It also means that $DB| \equiv DB \overset{PID_R}{\Longleftrightarrow} R$, and we obtain that:

$$T| \equiv DB| \Rightarrow \left( DB \overset{PID_R}{\Longleftrightarrow} R \right),$$
$$T| \equiv DB| \equiv \left( DB \overset{PID_R}{\Longleftrightarrow} R \right).$$

$T$ believes that $DB$ is honest and competent, and $DB$ believes that the pseudonym $PID_R$ shared by $DB$ and $R$ is honest.

Applying the jurisdiction rule (J1): $\frac{P| \equiv P'| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$, and we obtain that:

$$T| \equiv DB \overset{PID_R}{\Longleftrightarrow} R$$

If $T$ believes that $DB$ has jurisdiction over a statement, then $T$ trusts $DB$ on the truth of the statement. Thus, $T$ believes the pseudonym $PID_R$ is shared as a secret by $DB$ and $R$, and G3 has been proven.

**Theorem 4** *$R$ believes the pseudonym $PID_T$ is shared as a secret by DB and T.*

*Proof* According to the secure communication channel between $R$ and $DB$, we obtain that:

$$R| \equiv DB| \Rightarrow (DB| \equiv *),$$
$$R| \equiv DB| \equiv (DB| \equiv *).$$

Similarly, according to IA3.1 and J1, we obtain that:

$$DB| \equiv DB \overset{PID_T}{\Longleftrightarrow} T,$$
$$R| \equiv DB| \Rightarrow (DB \overset{PID_T}{\Longleftrightarrow} T),$$
$$R| \equiv DB \overset{PID_T}{\Longleftrightarrow} T.$$

Thus, $R$ believes the pseudonym $PID_T$ is shared by $DB$ and $T$, and G4 has been proven.

**Theorem 5** *$R$ believes that the value $H_T$ is fresh.*

*Proof* According to M2: $R \triangleleft H_R$, it turns out that $R$ has received messages $H_R$, which is a hash value involving $TID_T, B_T$, and $r_R$). Thus, $R \triangleleft H_R$ can be regarded as follows.

$$R \triangleleft (r_R, *)$$

According to IA2.3: $R| \equiv \sharp(r_R), R$ believes that $r_R$ is fresh. Applying the freshness rule (F1): $\frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X,Y)}$, we obtain that:

$$R| \equiv \sharp(r_R, *)$$

If one part of $H_R$ (marked as $(r_R, *)$) is known to be fresh, then $H_R$ are also fresh. Thus, $R$ will believe that the message $H_R$ is fresh ($R| \equiv \sharp(H_R)$), and G5 has been proven.

**Theorem 6** *$DB$ believes that $T$ once sent a message including the statement $Q$.*

*Proof* According to M3: $DB \triangleleft TID_T, DB$ receives the message $TID_T$. Here, $TID_T$ is computed involving $PID_T, B_T$ and $r_R$, in which $B_T = \mathcal{T}_z(Q)$. Thus, $DB \triangleleft TID_T$ can be regarded as follows.

$$DB \triangleleft (\langle Q \rangle_{PID_T}, *)$$

Applying the seeing rule (R1): $\frac{P \triangleleft (X,Y)}{P \triangleleft X}$, we obtain that:

$$DB \triangleleft \langle Q \rangle_{PID_T}$$

According to IA3.1: $DB| \equiv T \overset{PID_T}{\Longleftrightarrow} DB, DB$ believes that the secret $PID_T$ is shared with $t$. Applying the message-meaning rule (RM3): $\frac{P| \equiv P' \overset{Y}{\longleftrightarrow} P, P \triangleleft \langle X \rangle_Y}{P| \equiv P'| \sim X}$, we obtain that:

$$DB| \equiv T| \sim Q$$

If $DB$ believes that $PID_T$ is a shared secret with $R$, and $DB$ receives $\langle Q \rangle_{PID_T}, DB$ will believe that $T$ once conveyed the message $Q$. Till now, G6 has been proven, and G7 can also be achieved via the similar procedures.

In summary, the BAN logic based security proof is demonstrated for formal analysis. In C2MP, $R$, $T$, and $DB$ can, respectively, establish beliefs via the authentication, and the C2MP is proved to be correct and ensures nonexistence of obvious design defects.

## 5 Performance analysis

In performance analysis, the C2MP is investigated from three aspects: storage requirement, communication overhead and computation load.

- *Storage requirement* In the C2MP, $T/R$ stores the tag/reader real identifier $ID_T/ID_R$, pseudonym $PID_T/PID_R$, and the shared secrets $\{Q, S, p\}$. A 64-bit length is assumed for $ID_*$ and $PID_*$ according to ISO/IEC related standard. Additional memory consumption on PRNG and Chebyshev polynomials is necessary during protocol execution. In the C2MP, $DB$ can be regarded as a resource-rich entity, which stores all the legal tags/readers' real identifiers and pseudonyms. Note that an efficient implementation of hash functions (e.g. MD5, SHA-1, SHA-256) could be introduced with 16.0K–23.0K gates requirement [21].
- *Communication overhead* Communication overhead is the number of transmitted bit stream for each phase or for a full run of the protocol. In the C2MP, the number of transmitting frames depends on message exchanges in authentication phases. The communication overhead refers to the sum of signaling loads during each authentication session. Suppose the Chebyshev polynomials have $L$-bit length, the pseudonyms of readers and tags have the same length 64-bit, the pseudo-random numbers have 16-bit length, and the hash values have 128-bit length. The total length of message deliveries between a reader and a tag are $(52 + 1/4L)$ bytes. The total authentication progress completed via 5 phases is acceptable in practical applications.
- *Computation load* During the entire round, $T$ performs two PRNG operations, three Chebyshev polynomials $\mathcal{T}_z(.)$, one XOR bitwise operations, and three hash functions. $R$ performs two PRNG operations, three Chebyshev polynomials $\mathcal{T}_y(.)$, two XOR bitwise operations, and four hash functions. There are no complex encryption operations in the C2MP. Based on the existing technology, smart cards (e.g. MIFARE Plus, and MIFARE DESFire) [22] comprise with microprocessor unit (MPU), storage units, and chip operating system (COS). They can efficiently support the required algebraic algorithms. The power-saving module should be considered to deal with multi-rounds of Chebyshev chaotic maps.

## 6 Conclusion

In this paper, a Chebyshev chaotic map-based authentication protocol is proposed to address the security issues in RFID systems. The proposed C2MP adopts authentication, anonymity, and session freshness mechanism to enhance security and privacy protection. Particularly, Chebyshev polynomial's semigroup and chaotic properties are introduced for identity authentication and anonymous transmission. Dual random numbers are generated to achieve session freshness and forward security, and one-way hash functions are adopted for data integrity. The C2MP is verified by BAN logic to provide that there is nonexistence of obvious design flaws and security errors. It indicates that the C2MP is suitable for universal RFID applications.



## References

1. Ning H, Liu H, Yang LT (2013) Cyberentity security in the Internet of things. Computer 46(4):46–53
2. Ning H (2013) Unit and ubiquitous Internet of things. CRC Press, Taylor & France Group, Boca Raton
3. Zeng H, Zhang J, Dai G, Gao Z, Haiyang Hu (2014) Security visiting: RFID-based smartphone indoor guiding system. Int J Distrib Sens Netw 2014:1–13
4. Xie L, Yin Y, Vasilakos AV, Lu S (2014) Managing RFID data: challenges, opportunities and solutions. IEEE Commun Surv Tutor 16(3):1294–1311
5. Tian Y, Chen G, Li J (2012) A new ultralightweight RFID authentication protocol with permutation. IEEE Commun Lett 16(5):702–705
6. Liu H, Ning H, Zhang Y, He D, Xiong Q, Yang LT (2013) Grouping-proofs-based authentication protocol for distributed RFID systems. IEEE Trans Parallel Distrib Syst 24(7):1321–1330
7. Liu H, Ning H (2011) Zero-knowledge authentication protocol based on alternative mode in RFID systems. IEEE Sens J 11(12):3235–3245
8. Liu Z, Liu D, Li L, Lin H, Yong Z (2015) Implementation of a new RFID authentication protocol for EPC Gen2 standard. IEEE Sens J 15(2):1003–1011
9. Yao Q, Han J, Qi S, Liu Z, Chang S, Ma J (2013) MAP: towards authentication for multiple tags. Int J Distrib Sens Netw 2013:1–14
10. Avoine G, Kim CH (2013) Mutual Distance bounding protocols. IEEE Trans mob Comput 12(5):830–839
11. Morshed MM, Atkins A, Yu H (2012) Efficient mutual authentication protocol for radio frequency identification systems. IET Commun 6(16):2715–2724
12. Lu L, Han J, Hu L, Ni LM (2012) Dynamic key-updating: privacy-preserving authentication for RFID systems. Int J Distrib Sens Netw 2012:1–12
13. Ning H, Liu H, Mao J, Zhang Y (2011) Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. IET Commun 5(12):1755–1768
14. Jiang Y, Cheng W, Du X (2014) Group-based key array authentication protocol in radio frequency identification systems. IET Inf Secur 8(6):290–296
15. Avoine G, Bingol MA, Carpent X, Yalcin SBO (2013) Privacy-friendly authentication in RFID systems: on sublinear protocols based on symmetric-key cryptography. IEEE Trans Mob Comput 12(10):2037–2049
16. Hermans J, Peeters R, Preneel B (2014) Proper RFID privacy: model and protocols. IEEE Trans Mob Comput 13(12): 2888–2902 1
17. Ning H, Liu H, Yang LT (2014) Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Trans Parallel Distrib Syst. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6767153
18. Mason JC, Handscomb DC (2003) Chebyshev polynomials. Chapman & Hall/CRC Press, Boca Raton
19. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 37(3): 669–674
20. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
21. http://www.heliontech.com/core.htm. Accessed Dec (2014)
22. http://www.nxp.com. Accessed Dec (2014)